ABSTRACT OF THE DISCLOSURE

Computer-based methods and systems for automatically protecting a storage device from unwanted alterations are provided. Example embodiments provide a Disk Access Redirection System, which includes a Redirection Driver, an Available Space Table ("AST"), a Protected Space Redirection Table ("PSRT"), and optionally an Unprotected Space Table ("UST"). The Redirection Driver is installed and registered with the computer operating system so that it can intercept storage device access requests (such as a disk read / write). When a storage access request for a read or a write is sent, the request is intercepted by the Redirection Driver, transparent to the code that invokes the storage access request. Upon intercepting a write request, the Redirection Driver determines whether the target location is protected (using the PSRT and UST). If so, the Redirection Driver writes to a redirected data area, allocating more space to the redirected data area as needed. Upon intercepting a read request, the Redirection Driver determines whether to read data from the specified source location or whether to translate the request to read data from the redirected data area to which the source location has been previously redirected. The Redirection Driver uses the AST, PSRT, and optionally the UST, to allocate available storage space for redirected write requests, redirect write requests for protected areas of the storage device, and redirect read requests when the read request specifies a storage location that has been previously redirected. A Redirection Driver can be implemented to intercept storage access requests at different levels of storage access, including files, clusters, logical sectors, physical sectors, or at any defined data abstraction level. When the computer system is shut down, the redirected data area is discarded, thereby automatically reinstating the original state of the storage device when the computer is rebooted.

470039.401\401-AP\203001_1